

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282991

(43)Date of publication of application : 15.10.1999

(51)Int.Cl.

G06K 19/07

G06F 3/08

G06K 17/00

G06K 19/073

(21)Application number : 10-083468

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 30.03.1998

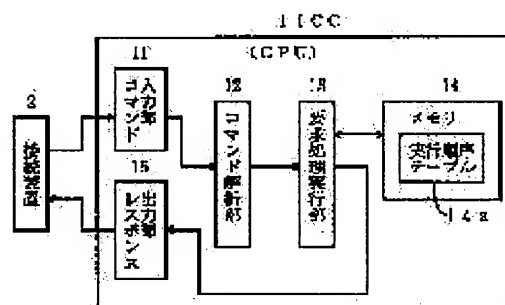
(72)Inventor : MORIYAMA AKIKO

(54) IC CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To process a command as an error unless it is transmitted in previously decided order and to prevent illegal usage by providing a table where instruction executing order is registered in a non-volatile memory.

SOLUTION: An IC card(ICC) 1 is provided with an execution order table 14a for defining the execution order of commands in a memory 14. Each command for supporting ICC 1 has a unique command number, the execution order is registered in the table 14a by using the command number, the command which agrees with the registered execution order is properly processed and the command which does not agree is adopted as the error. When ICC 1 supports the three commands, that is, a reading command, a writing command and an erasing command, for example, the command numbers 01-03 are respectively assigned and, moreover, 04 is assigned to an authenticating command. The order is previously registered in the table 14a by using the command numbers.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-282991

(43) 公開日 平成11年(1999)10月15日

(51) IntCl.⁸

識別記号

F I

G 0 6 K 19/07

G 0 6 K 19/00

N

G 0 6 F 3/08

G 0 6 F 3/08

C

G 0 6 K 17/00

G 0 6 K 17/00

B

E

19/073

19/00

P

審査請求 未請求 請求項の数 3 O L (全 5 頁)

(21) 出願番号

特願平10-83468

(22) 出願日

平成10年(1998)3月30日

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 森山明子

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

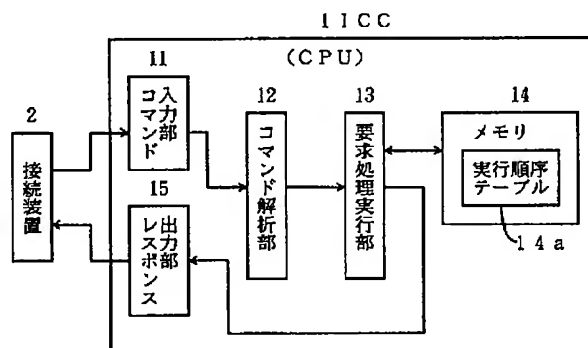
(74) 代理人 弁理士 蛭川 昌信 (外7名)

(54) 【発明の名称】 ICカード

(57) 【要約】

【課題】 予め定められた順序でコマンドが送信されない場合はエラーにして不正な使用を防ぐ。

【解決手段】 命令入力部11、応答出力部15、命令解析部12、命令処理実行部13、データを記憶する不揮発性メモリ14を備えたICカードにおいて、不揮発性メモリ14に命令の実行順序を登録したテーブル14aを備えたものである。



【特許請求の範囲】

【請求項 1】 命令入力部、応答出力部、命令解析部、命令処理実行部、データを記憶する不揮発性メモリを備えた IC カードにおいて、不揮発性メモリに命令の実行順序を登録したテーブルを備えたことを特徴とする IC カード。

【請求項 2】 請求項 1 記載の IC カードにおいて、各命令が実行順序を示す番号を備えたことを特徴とする IC カード。

【請求項 3】 請求項 1 記載の IC カードにおいて、認証が成立したことを条件に、前記テーブルに規定された実行順序を書き換えることができる専用の命令を有することを特徴とする IC カード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は IC カード（IC C）に関する。

【0002】

【従来の技術】近年、クレジットカードやプリペイドカード等さまざまな形で IC C が使用され、CPU を内蔵して利便性の観点からいろいろな機能が付加されて汎用性を持たせたものが開発されている。このような従来の IC C についてその概略を説明する。図 8 において、CPU を内蔵した IC C 1 は、接続装置 2（インターフェース・デバイス：IFD）からの処理要求であるコマンド（命令）を受け付けるコマンド入力部 11、受け付けたコマンドを解析するコマンド解析部 12、解析したコマンドに基づき要求されている処理を実行する要求処理実行部 13、処理の実行過程においてアクセスされるメモリ 14、処理結果をレスポンスとして接続装置 2 へ返すレスポンス出力部とからなっている。

【0003】接続装置 2 と IC C 1 の間で交換される情報（コマンド、レスポンス）の最小単位はキャラクタであり、図 9 に示すように、先頭からスタートビット（ST）、8 個のデータビット（a～h）・パリティビット（i）の順に送信され、直後にキャラクタ保護時間（GT）が 1 ビット以上続く形になっている。

【0004】このようなキャラクタ複数個から、例えば T=1 ブロック伝送プロトコルを利用する場合、図 10 に示すような情報ブロックが構成される。情報ブロックは、先頭フィールド、情報フィールド（INF）、最終フィールドからなり、先頭フィールドは、ブロックの送信元のアドレス、あて先アドレス及び VPP 端子の状態制御を示すノードアドレス（NAD）1 バイト、伝送制御情報を含むプロトコル制御バイト（PCB）1 バイト、および情報フィールド長（LEN）1 バイトからなり、情報フィールドは、最大 254 バイトまで挿入可能であり、ブロックの最後は必ず誤り検出符合（EDC）1 または 2 バイトとなる。なお、各 1 バイトには、実際には ST ビット、パリティ検査ビット、GT が付加され

ている。

【0005】接続装置 2 から IC C 1 に送られるコマンドは図 10 に示すブロックの情報フィールド内に収められ、図 11 に示すように、見出し部と本体部から構成される。見出し部は、ISO のコマンドか否かを示すクラスバイト（CLA）、命令コード（INS）、アクセスするファイルを指示するパラメータ P1、P2 からなり、本体部はコマンドデータフィールドバイト長（Lc）、コマンドデータフィールド（c データ：可変長）、レスポンスデータフィールド長（Le）からなっている。

【0006】また、IC C 1 から接続装置 2 へ送られるレスポンスは、図 12 に示すように、本体部、後続部からなり、先頭からレスポンスデータフィールド（r データ）、処理結果を示すステータスデータバイト 1（SW1）、ステータスデータバイト 2（SW2）の順に送られる。

【0007】

【発明が解決しようとする課題】ところで、IC C ではその内部で実行するコマンドのシーケンス（順序）に関してほとんどチェック機能を持たず、外部システム（接続装置）側での管理に任されていた。しかし、近年では偽造 IC カードや偽造端末による不正を防ぐために IC カード利用シーケンスを監視する機能が IC カード側にも必要になってきた。

【0008】本発明は上記課題を解決するためのもので、IC カード内にチェック機構を設け、予め定められた順序でコマンドが送信されない場合はエラーとして処理することにより、不正な使用を防ぐことを目的とするものである。

【0009】

【課題を解決するための手段】本発明は、命令入力部、応答出力部、命令解析部、命令処理実行部、データを記憶する不揮発性メモリを備えた IC カードにおいて、不揮発性メモリに命令の実行順序を登録したテーブルを備えたことを特徴とする。また本発明は、各命令が実行順序を示す番号を備えたことを特徴とする。また本発明は、認証が成立したことを条件に、前記テーブルに規定された実行順序を書き換えることができる専用の命令を有することを特徴とする。

【0010】

【発明の実施の形態】以下、本発明の実施の形態について説明する。図 1 は本発明の IC C を説明する図であり、図 8 と同一参照数字は同一内容を示している。図 2 は本発明において用いられるコマンドの構成を説明する図、図 3 は使用されるコマンドの例を説明する図、図 4 は実行順序テーブルを説明する図である。図 1 に示す IC C は、メモリ 14 内にコマンドの実行順序を規定する実行順序テーブル 14a を備えた以外は図 8 で説明したものと同一であるので、その詳細な説明は省略する。本

発明においては、I C C のサポートするコマンドそれぞれがユニークなコマンド番号を持ち、その実行順序がコマンド番号を使ってテーブル 1 4 a に登録されており、登録された実行順序に合致するコマンドは適正に処理され、それに合致しないコマンドはエラーとなる。

【0 0 1 1】例えば、I C C が 3 つのコマンド、R E A D (読取り) コマンド、W R I T E (書き込み) コマンド、E R A S E (消去) コマンドをサポートしているとすると、図 3 に示すようにそれぞれにコマンド番号 0 1、0 2、0 3 が割当られ、さらに V E R I F Y (認 10 証) コマンドには 0 4 を割り当てる。このコマンド番号を利用して実行順序テーブル 1 4 a には予めその順番が登録されている。コマンド番号はコマンドコード (I N S) を利用するのがよい。

【0 0 1 2】図 4 (a) は実行順序テーブルの 1 例を示すもので、リセット (活性化) 直後のコマンドにのみ適用するの可否かのフラグが O N になっている場合を例に説明する。このフラグは、図 4 (b) に示すように、0 0 の場合はリセット直後のコマンドに適用、0 1 の場合はリセット直後のコマンド以外にも適用するものである。 20 ももちろんこのような規定をせず、常時コマンド順序が適用されるようにしてもよい。この例では、1 コマンド目がコマンド番号 0 3、2 コマンド目がコマンド番号 0 2 となっている場合に正常処理が行われ、これ以外の順番ではエラーとなる。すなわち、1 コマンド目に記載されているコマンドを受信すると、次のコマンドは 2 番目に指定されているコマンド以外は受付なくなり、I C C からはエラーステータスが返される。こうして誤ったコマンドシーケンスによる利用を防止することができる。なお、番号を付して前後の順番を間違わないようにする 30 コマンドは、特に重要なコマンドに対して行うようにしても良く、また番号を付すコマンドの数はテーブルの許す範囲で広げることができる。

【0 0 1 3】図 5 は実行順序指定によるコマンド処理の 1 例を示す処理フローであり、この処理では送信されるコマンド 1 つ 1 つについての処理を実行し、順番が間違 40 った段階でエラーステータスを返すものである。I C C を活性化し、外部から I C C へコマンドが送信されると、I C C ではコマンド受信処理を行う (ステップ S 1 ~ S 3)。次いで、I C C では図 4 (b) に示したフラグのチェックを行い、フラグがセットされているかを判断する (ステップ S 4、S 5)。フラグがセットされている場合は、リセット直後のコマンドにのみ適用されるため、リセット直後のコマンドか否かを判断し、リセット直後のコマンドであれば、テーブルチェックを行い、また、ステップ S 5 でフラグがリセットされている場合はリセット直後以外のコマンドにも適用されるためテーブルチェックを行う (ステップ S 6、S 7)。テーブルチェックを行ってコマンド実行順序が一致している場合、あるいはステップ S 6 でリセット直後のコマンド 50

でない場合は、そのままコマンド処理を実行し (ステップ S 9)、I C C から正常な処理が行われたことを接続装置へレスポンスとして返し (ステップ S 1 0)、以上の処理が最後のコマンドまで実行される (ステップ S 1 1)。また、ステップ S 8 において、テーブルに登録した実行順序と不一致の場合には、その時点でレスポンス処理でエラーステータスを返し処理を終了する。

【0 0 1 4】前述したように、コマンドの実行順序は不揮発性メモリにテーブルとして登録されているが、この 10 実行順序は専用のコマンドを用いて I C C 発行処理後に変更するようにしてもよく、そうした例について以下に説明する。図 6 は実行順序テーブルを書き換える専用のコマンドの構成を示し、例えば命令コードが 9 9 の場合はこの専用のコマンドとする。専用コマンドのデータ部の 0 0 は図 4 (b) で示したフラグに相当し、このコマンドではリセット直後に適用することを示している。次の 2 バイトの 0 1、0 2 はコマンドの実行順序を示している。こうしてリセット直後に適用可否かのフラグと、コマンド実行順序が新たに書き換えられる。なお、この 20 コマンドは認証処理が成功したときのみ行えることとし、正当な権利を持つ人以外は実行できないようにしておく必要がある。

【0 0 1 5】図 7 は実行順序テーブルを書き換える処理を説明する図である。I C C を活性化し、外部から I C C へコマンドを送信し、I C C 側でコマンド受信処理を行う (ステップ S 4 1 ~ S 4 3)。次いで、認証処理を実行し (ステップ S 4 4)、認証 O K か否かを判断し (ステップ S 4 5)、認証が成功しなかった場合には処理は 30 終了する。認証が成功した場合には命令コードを見て、順序テーブル書き換えコマンドか否かを判断する (ステップ S 4 6)。順序テーブル書き換えコマンドでない場合は処理は終了する。順序テーブル書き換えコマンドの場合には、リセット直後に適用するフラグをセットするの可否かを判断し (ステップ S 4 7)、セットの場合にはフラグセット処理、セットでない場合はフラグリセット処理をそれぞれ行い (ステップ S 4 8、4 9)、次いで、順序テーブル書き換え処理を実行する (ステップ S 5 0)。こうして認証が成功した正当な権利を持つ人のみがフラグセット処理、実行順序テーブル書き換え処理を行うことができる。

【0 0 1 6】

【発明の効果】以上のように本発明によれば、I C カード内にチェック機構を設け、I C カード内の機能を利用する時には、予め定められた手順に従ってコマンドを I C カードへ送らなければ違反と見なしエラーステータスが返されるので、誤ったコマンドシーケンスの利用を防止し、偽造 I C カードや偽造端末による不正利用を防ぐことが可能となる。

【図面の簡単な説明】

【図 1】 本発明の I C カードを説明する図である。

【図 2】 本発明のコマンドの構成を説明する図である。

【図 3】 本発明で使用するコマンドの例を説明する図である。

【図 4】 実行順序テーブルを説明する図である。

【図 5】 順序指定によるコマンド処理の 1 例を示す処理フローを示す図である。

【図 6】 実行順序テーブルを書き換える専用のコマンドの構成を示す図である。

【図 7】 実行順序テーブルを書き換える処理を説明する

* 図である。

【図 8】 従来の ICC を説明する概略図である。

【図 9】 キャラクタを説明する図である。

【図 10】 ブロックを説明する図である。

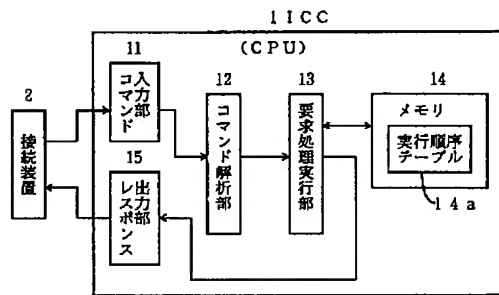
【図 11】 コマンドを説明する図である。

【図 12】 レスポンスを説明する図である。

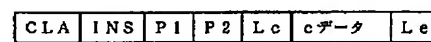
【符号の説明】

1…IC カード、2…接続装置、12…コマンド解析部、13…コマンド処理実行部、14…メモリ、14a…実行順序テーブル。

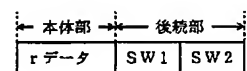
【図 1】



【図 2】



【図 12】



【図 6】

CLA	INS	P1	P2	Lc	データ
9 0	9 9	0 0	0 0	0 3	0 0 0 1 0 2

【図 3】

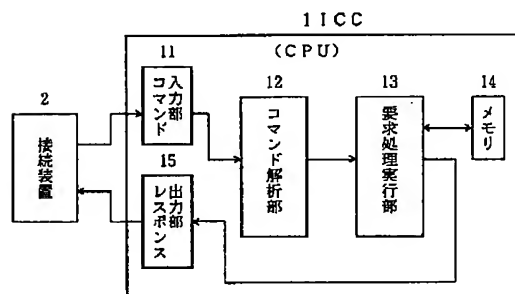
コマンド番号	コマンド名
0 1	READコマンド
0 2	WRITEコマンド
0 3	ERASEコマンド
0 4	VERIFYコマンド

【図 4】

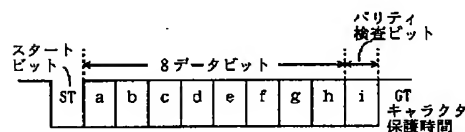
リセット直後のコマンドに適用	1 コマンド目	2 コマンド目
ON	0 3	0 2

0 0	リセット直後のコマンドに適用
0 1	リセット直後のコマンド以外に適用

【図 8】



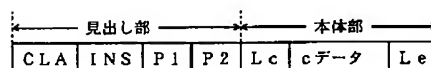
【図 9】



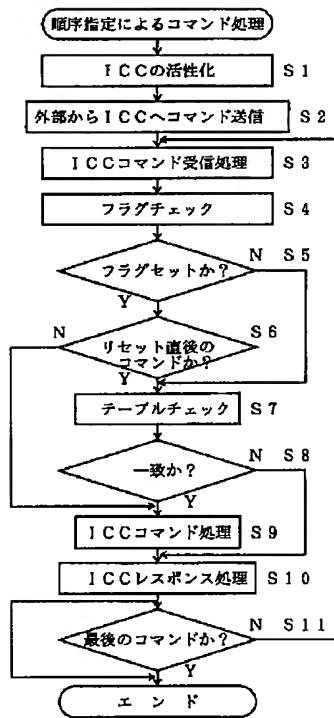
【図 10】

先頭フィールド	情報フィールド	最終フィールド
NAD 1 バイト	PCB 1 バイト	LEN 1 バイト
	INF 0 ~ 2 5 4 バイト	EDC 1 又は 2 バイト

【図 11】



【図5】



【図7】

